

# Teams/Groups

Name	Email Address	Team
Dai, Yahan	tut06385@temple.edu	1
Dong, Fang	tut06980@temple.edu	1
Guo, Baowei	tus93976@temple.edu	1
Guo, Mengfan	mguo@temple.edu	1
Hou, Yucheng	tut00371@temple.edu	1
Jiang, Jingyu	tut09033@temple.edu	2
Li, Ao	tus97456@temple.edu	2
Li, Chaoyue	tus93469@temple.edu	2
Li, Menghe	tus94160@temple.edu	2
Lin, Zhichao	tus97675@temple.edu	2
Liu, Dongchang	tus93533@temple.edu	3
Luo, Yusen	tus93022@temple.edu	3
Qiao, Weifan	tut06871@temple.edu	3
Que, Yifei	tut04639@temple.edu	3
Shao, Kang	tus93718@temple.edu	3
Tian, Zijian	tus99737@temple.edu	4
Wan, Ziyi	tut06981@temple.edu	4
Wang, Qian	tus93017@temple.edu	4
Wang, Yihan	tus94162@temple.edu	4
Wu, Jianan	tut04640@temple.edu	4
Wu, Yimo	tut09063@temple.edu	5
Xue, Luxiao	tut04749@temple.edu	5
Yang, Yifan	tus93035@temple.edu	5
Yin, Yuqing	yyin@temple.edu	5
Zhang, Tongjia	tut04636@temple.edu	5
Zhang, Xiinyue	tut09069@temple.edu	6
Zhao, Wenhan	tus93018@temple.edu	6
Zheng, Yi	tus93539@temple.edu	6
Zhi, Ruoyu	tut04744@temple.edu	6
Zhao, Ao	tus93195@temple.edu	6

# Unit #0b

# Threat Environment

MIS5214 – Security Architecture

## Unit 0b – The Threat Environment

### Readings

- Boyle and Panko: Chapter 1 The Threat Environment
- Ross, J.W., Weill P, and Robertson D.C. (2008), "Implement the Operating Model Via Enterprise Architecture" (in the [Harvard Business Publishing course pack](#))
- [NIST SP 800-100 "Information Security Handbook: A Guide for Managers"](#), Chapter 10 Risk Management pp.84-95

# Agenda

- Terminology
- Threat environment
- Hacker mindset
- More terminology
- Security architecture
- Next steps...

# Introductory Terminology

***“Information security” is protection of...***

- Confidentiality, integrity, and availability (“CIA”) of data and information
- Data, information and information systems from unauthorized...
  - Access, use, disclosure = **Confidentiality**
  - Modification = **Integrity**
  - Disruption or destruction = **Availability**



# Terminology: Security Goals

# Confidentiality

Confidentiality means that people cannot read sensitive information, either while it is on a computer or while it is traveling across a network

## Examples of Threats:

- Data breaches (e.g., unauthorized access to financial records)
- Insider threats leaking confidential information
- Eavesdropping attacks (e.g., MITM attacks)

## Protection Mechanisms:

- Encryption (e.g., AES, TLS for secure communication)
- Access controls (e.g., Role-Based Access Control (RBAC))
- Multi-Factor Authentication (MFA)
- Data classification and handling policies

# Integrity

- Integrity means that attackers cannot change or diminish information, either while it is on a computer or while it is traveling across a network
- Or, at least, if information is changed or diminished, then the receiver can detect the change and possibly restore the data

## Examples of Threats:

- Unauthorized modifications (e.g., altering financial transactions)
- Data corruption (e.g., malware modifying critical system files)
- Man-in-the-Middle (MITM) attacks altering data in transit

## Protection Mechanisms:

- Hashing and Checksums (e.g., SHA-256 for file verification)
- Digital signatures (e.g., signing emails or software updates)
- Access control lists (ACLs)
- Data backup strategies to recover original data



# Availability

- People who are authorized to use information are not prevented from doing so

## Examples of Threats:

- Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks
- Ransomware attacks encrypting files and making them unavailable
- Hardware failures and natural disasters impacting services

## Protection Mechanisms:

- Redundant systems and failover mechanisms
- Regular data backups and disaster recovery plans
- DDoS protection services and network load balancing
- Patch management to prevent security exploits

# Terminology: Compromises

- Successful attacks
- Also called incidents
- Also called breaches (not breeches)



# Terminology: Countermeasures


- Tools used to thwart attacks
- Also called safeguards, protections, and controls
- Types of countermeasures
  - Preventative
  - Detective
  - Corrective

# Agenda

- ✓ Terminology
- Threat environment
- More terminology
- Security architecture
- Next steps...

# The Threat Environment

NIST SP 800-30r1 “Guide for Conducting Risk Assessments”, page 66

Type of Threat Source	Description	Characteristics
<b>ADVERSARIAL</b> <ul style="list-style-type: none"> <li>- Individual <ul style="list-style-type: none"> <li>- Outsider</li> <li>- Insider</li> <li>- Trusted Insider</li> <li>- Privileged Insider</li> </ul> </li> <li>- Group <ul style="list-style-type: none"> <li>- Ad hoc</li> <li>- Established</li> </ul> </li> <li>- Organization <ul style="list-style-type: none"> <li>- Competitor</li> <li>- Supplier</li> <li>- Partner</li> <li>- Customer</li> <li>- Nation-State</li> </ul> </li> </ul>	<p>Individuals, groups, organizations, or states that seek to exploit the organization's dependence on cyber resources (i.e., information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies).</p> 	<p>Capability, Intent, Targeting</p>
<b>ACCIDENTAL</b> <ul style="list-style-type: none"> <li>- User</li> <li>- Privileged User/Administrator</li> </ul>	<p>Erroneous actions taken by individuals in the course of executing their everyday responsibilities.</p>	<p>Range of effects</p>
<b>STRUCTURAL</b> <ul style="list-style-type: none"> <li>- Information Technology (IT) Equipment <ul style="list-style-type: none"> <li>- Storage</li> <li>- Processing</li> <li>- Communications</li> <li>- Display</li> <li>- Sensor</li> <li>- Controller</li> </ul> </li> <li>- Environmental Controls <ul style="list-style-type: none"> <li>- Temperature/Humidity Controls</li> <li>- Power Supply</li> </ul> </li> <li>- Software <ul style="list-style-type: none"> <li>- Operating System</li> <li>- Networking</li> <li>- General-Purpose Application</li> <li>- Mission-Specific Application</li> </ul> </li> </ul>	<p>Failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances which exceed expected operating parameters.</p>	<p>Range of effects</p>
<b>ENVIRONMENTAL</b> <ul style="list-style-type: none"> <li>- Natural or man-made disaster <ul style="list-style-type: none"> <li>- Fire</li> <li>- Flood/Tsunami</li> <li>- Windstorm/Tornado</li> <li>- Hurricane</li> <li>- Earthquake</li> <li>- Bombing</li> <li>- Overrun</li> </ul> </li> <li>- Unusual Natural Event (e.g., sunspots)</li> <li>- Infrastructure Failure/Outage <ul style="list-style-type: none"> <li>- Telecommunications</li> <li>- Electrical Power</li> </ul> </li> </ul>	<p>Natural disasters and failures of critical infrastructures on which the organization depends, but which are outside the control of the organization.</p> <p>Note: Natural and man-made disasters can also be characterized in terms of their severity and/or duration. However, because the threat source and the threat event are strongly identified, severity and duration can be included in the description of the threat event (e.g., Category 5 hurricane causes extensive damage to the facilities housing mission-critical systems, making those systems unavailable for three weeks).</p>	<p>Range of effects</p>

# Adversarial (i.e. purposeful) threat sources

Type of Threat Source	Description	Characteristics
<p>ADVERSARIAL</p> <ul style="list-style-type: none"><li>- Individual<ul style="list-style-type: none"><li>- Outsider</li><li>- Insider</li><li>- Trusted Insider</li><li>- Privileged Insider</li></ul></li><li>- Group<ul style="list-style-type: none"><li>- Ad hoc</li><li>- Established</li></ul></li><li>- Organization<ul style="list-style-type: none"><li>- Competitor</li><li>- Supplier</li><li>- Partner</li><li>- Customer</li></ul></li><li>- Nation-State</li></ul>	<p>Individuals, groups, organizations, or states that seek to exploit the organization's dependence on cyber resources (i.e., information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies).</p>	<p>Capability, Intent, Targeting</p>

NIST SP 800-30r1 “Guide for Conducting Risk Assessments”, page 66



# What type of Hacker are you?



*“You need to decide if you’re going to aspire to safeguarding the common good or settle for pettier goals. Do you want to be a mischievous, criminal hacker or a righteous, powerful defender?”*

*...the best and most intelligent hackers work for the good side. They get to exercise their minds, grow intellectually, and not have to worry about being arrested. They get to work on the forefront of computer security, gain the admiration of their peers, further human advancement in the name of all that is good, and get well paid for it.”*

Grimes, R. (2017), Hacking the Hacker, John Wiley and Sons

# Most Hackers Aren't Geniuses



*“...readers often assume” bad-guy hackers are super smart, “...because they appear to be practicing some advanced black magic that the rest of the world does not know. In the collective psyche of the world, it’s as if ‘malicious hacker’ and ‘super-intelligence’ have to go together.*

*A few are smart, most are average, and some aren’t very bright at all, just like the rest of the world. Hackers simply know some facts and processes that other people don’t, just like a carpenter, plumber, or electrician.”*

Grimes, R. (2017), Hacking the Hacker, John Wiley and Sons





# Defenders are Hackers Plus

*“If we do an intellectual comparison alone, the defenders on average are smarter than the attackers. A defender has to know everything a malicious hacker does plus how to stop the attack. And that defense won’t work unless it has almost no end-user involvement, works silently behind the scenes, and works perfectly (or almost perfectly) all the time.*

*Show me a malicious hacker with a particular technique, and I’ll show you more defenders that are smarter and better. It’s just that the attacker usually gets more press.”* It’s time for equal time for the defender!

Grimes, R. (2017), Hacking the Hacker, John Wiley and Sons

# Hackers are Special

While not all are super-smart, “they all share a few common traits:”

- Broad intellectual curiosity
- Willingness to try things outside the given interface or boundary
- Not afraid to make their own way
- Usually they are life hackers:
  - Hacking all sorts of things beyond computers
  - Questioning the status quo and exploring all the time
- Most useful trait:
  - Persistence
  - Malicious hackers look for defensive weaknesses
  - Both malicious hackers and defenders are looking for weaknesses, just from opposite sides of the system
  - Both sides participate in an ongoing war with many battles, wins and losses. The most persistent side wins

Grimes, R. (2017), Hacking the Hacker, John Wiley and Sons

# The Secret to Hacking

*“If there is a secret to how hackers hack, it’s that there is no secret to how they hack. It’s a process of learning the right methods and using the right tools for the job.... There isn’t even one way to do it. There is, however, a definitive set of steps that describe the larger, encompassing process”*

## **Hacking Methodology Model**

1. Information gathering (“reconnaissance”)
2. Penetration
3. *Optional: Guaranteeing future easier access*
4. Internal reconnaissance
5. *Optional: Movement*
6. Intended action execution (e.g. data exfiltration)
7. *Optional: Covering Tracks*

# Integrating Boyle & Panko's Threat Environment with NIST SP 800-100 Risk Management

## Threat Identification

- Identify internal and external threats
- Recognize potential attack vectors
- Use threat intelligence and historical data

### Boyle & Panko's Threat Environment:

- Cybercriminals, Hacktivists, Insiders
- Nation-state attackers
- Malware, Phishing, DDoS, Zero-days

## Risk Analysis

- Assess likelihood and impact of threats
- Identify vulnerabilities and security gaps
- Prioritize risks based on criticality

### Boyle & Panko's Attack Process:

- Reconnaissance (info gathering)
- Scanning (probing vulnerabilities)
- Exploitation (gaining access)
- Post-exploitation (maintaining access)
- Covering tracks (evading detection)

# Integrating Boyle & Panko's Threat Environment with NIST SP 800-100 Risk Management

## **Risk Mitigation**

- Apply Defense in Depth strategy
- Use the Principle of Least Privilege
- Implement continuous monitoring
- Establish an Incident Response Plan

### **Boyle & Panko's Defensive Strategies:**

- Security Awareness Training
- Zero Trust Architecture
- Network Segmentation and MFA
- Endpoint Protection (EDR, IDS/IPS)

## **Risk Management Trends**

- Adaptive risk management due to evolving threats
- AI and automation in threat detection
- Third-party and supply chain risk considerations

### **Boyle & Panko's Emerging Threats:**

- Ransomware-as-a-Service (RaaS)
- AI-powered cyberattacks
- Advanced Persistent Threats (APTs)

# Integrating Boyle & Panko's Threat Environment with NIST SP 800-100 Risk Management

**1.Threats drive risk management decisions** → Understanding attack vectors and adversaries helps assess and prioritize risks.

**1.Attack process aligns with risk analysis** → The way attackers operate informs how organizations identify vulnerabilities.

**1.Mitigation strategies reduce risk impact** → Defense-in-depth principles directly counteract identified threats.

**1.Emerging threats require evolving risk strategies** → AI, ransomware, and zero-day threats demand continuous adaptation.

# Anatomy of an Attack

(MANDIANT, 2015)

## Threat landscape

1. **Attacker sends spear phishing e-mail**

2. **Victim opens attachment**

- Custom malware is installed

3. **Custom malware communicates to control web site**

- Pulls down additional malware

4. **Attacker establishes multiple backdoors**

5. **Attacker accesses system**

- Dumps account names and passwords from domain controller

6. **Attacker cracks passwords**

- Has legitimate user accounts to continue attack undetected

7. **Attacker reconnaissance**

- Identifies and gathers data

8. **Data collected on staging server**

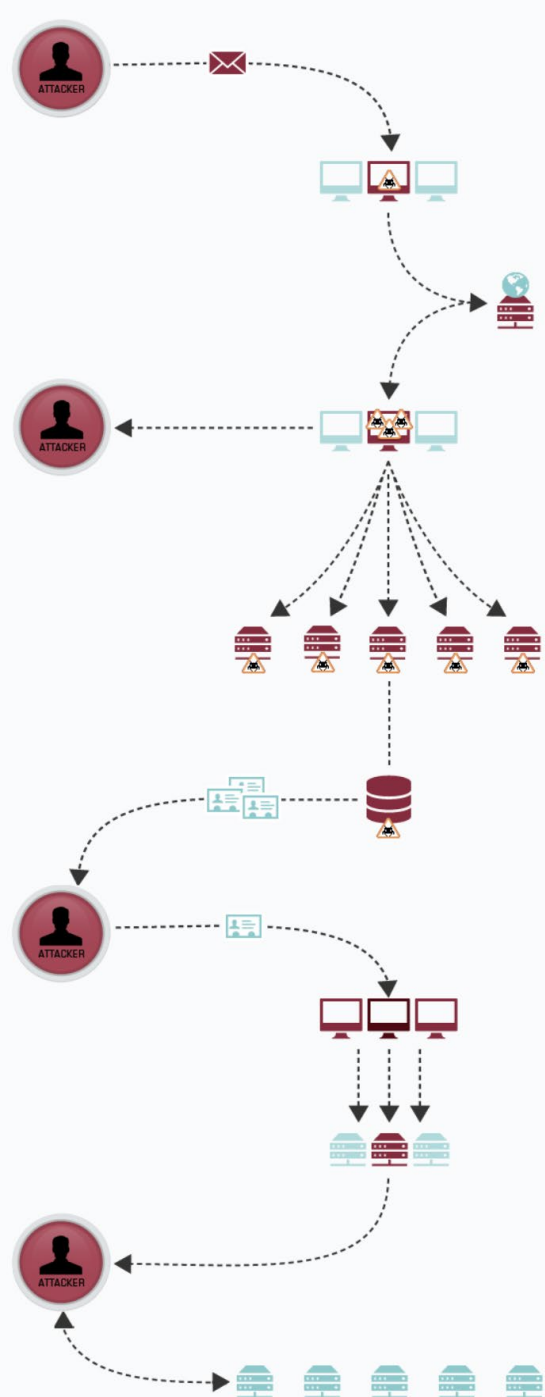
9. **Data ex-filtrated**

10. **Attacker covers tracks**

- Deletes files
- Can return any time

***Advanced persistent threats (APT) usually maintain remote access to target environments for 6-18 months before being detected (i.e. they are persistent)***

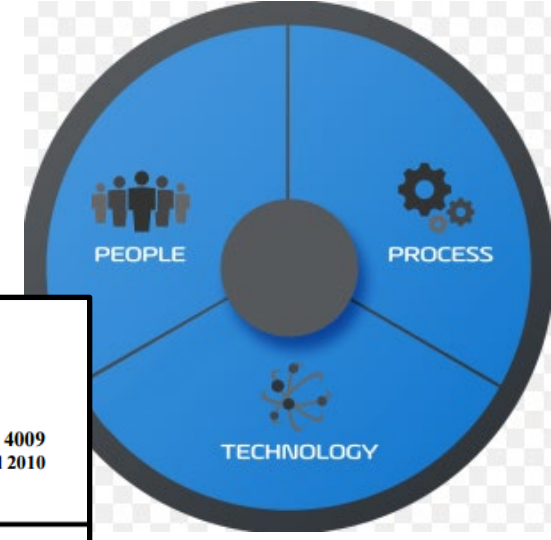
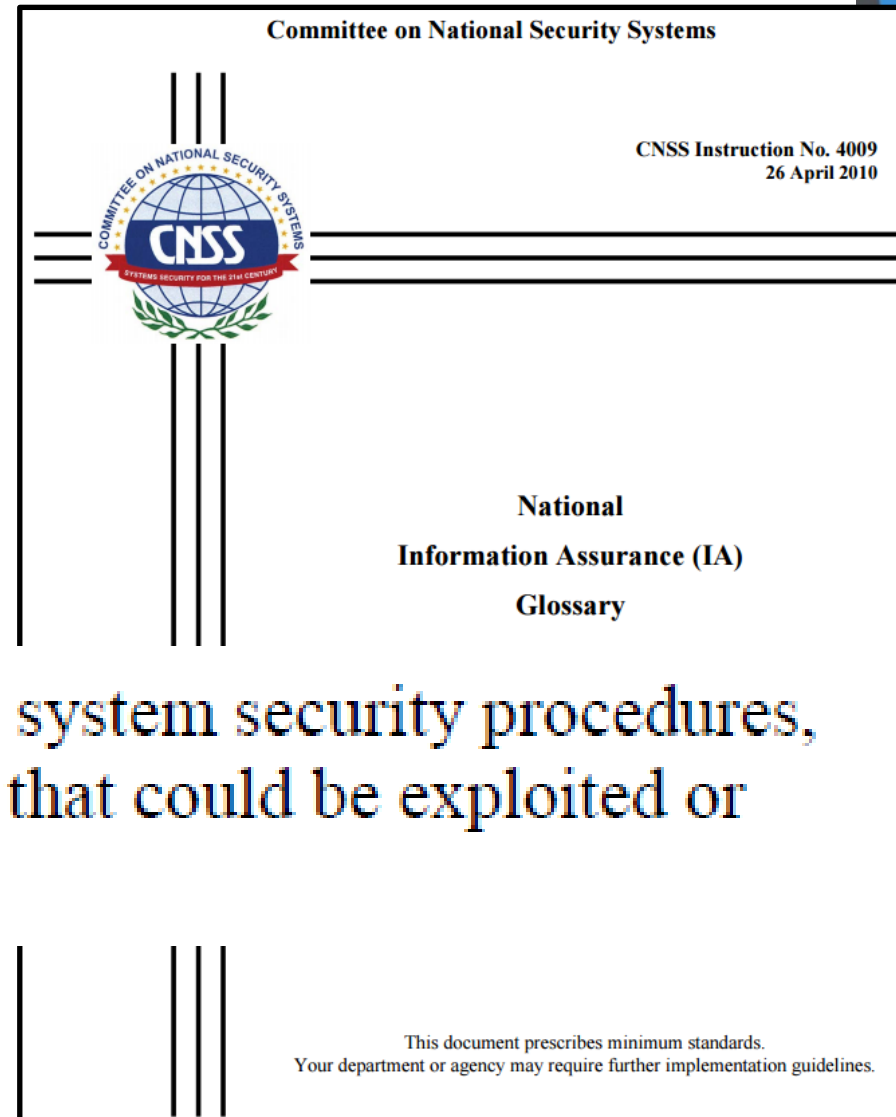
(Holcomb & Stapf, 2014)



# What is a Vulnerability?

*Any unaddressed susceptibility to a physical, technical or administrative information security threat*

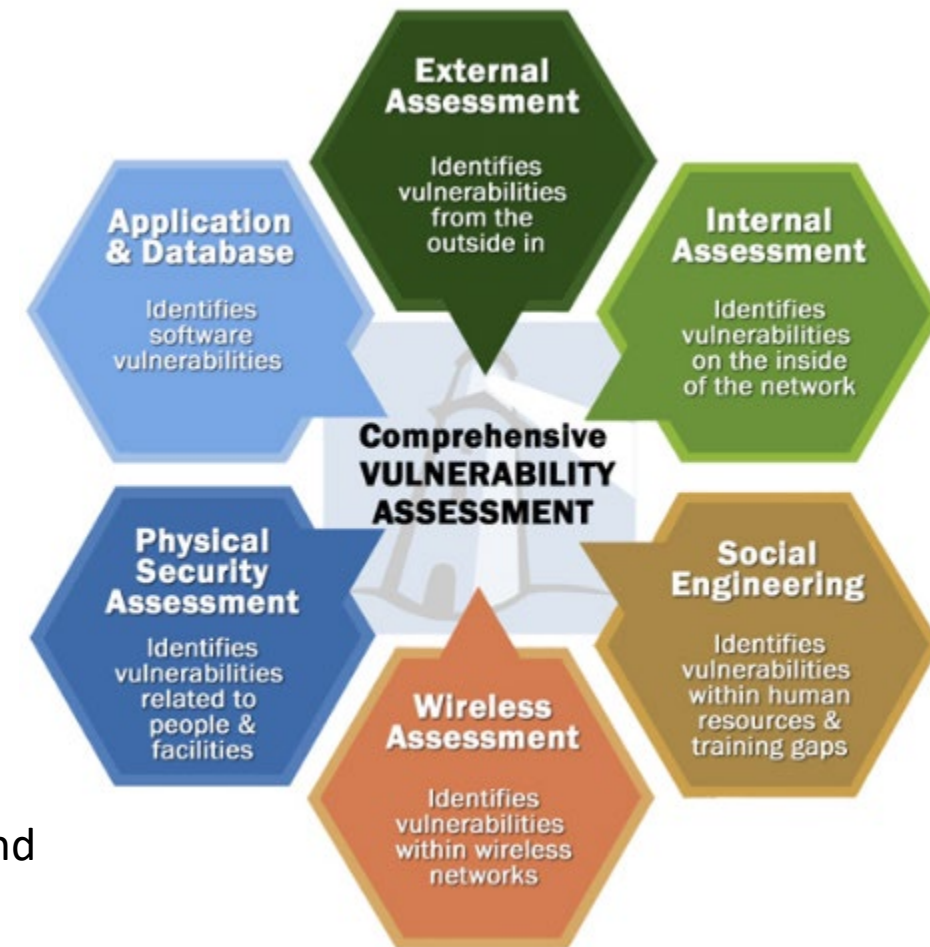
Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.





# Vulnerabilities can be classified by asset class

- Physical examples
  - Buildings in environmental hazard zones (e.g. low floor in flood zone)
  - Unlocked and unprotected doors to data center
  - Unreliable power sources
- Technical examples
  - Hardware – susceptibility to humidity, dust, soiling, unprotected storage
  - Software – insufficient testing, lack of audit trail, poor or missing user authentication and access control
  - Data – unencrypted transfer or storage, lack of backup
  - Network – Unprotected communication lines, insecure architecture
- Organizational examples
  - Inadequate screening and recruiting process, lack of security awareness and training
  - Lack of regular audits
  - Lack of security and IT related business continuity plans

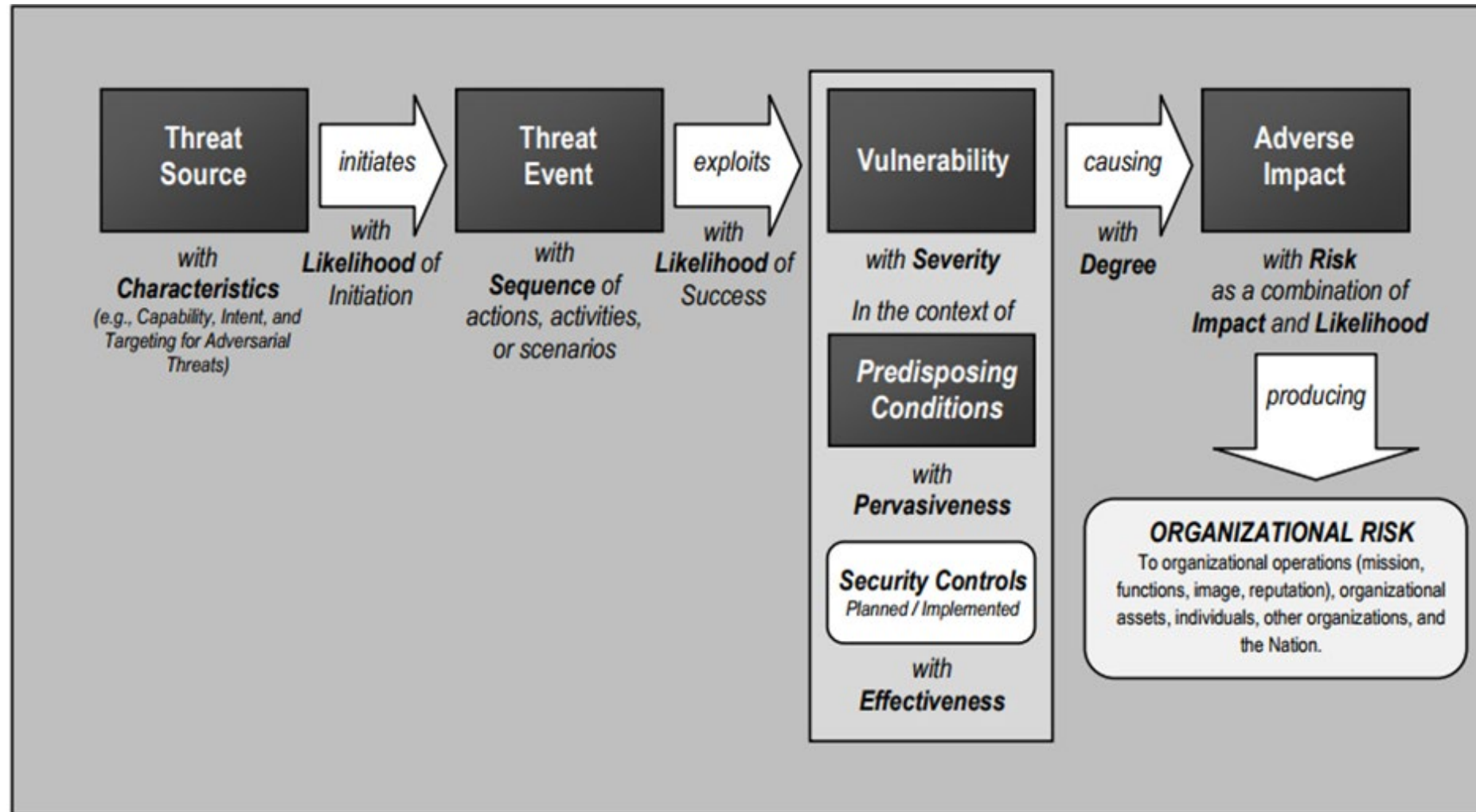


[http://www.infosightinc.com/collaterals/CVA-PT\\_March2016.pdf](http://www.infosightinc.com/collaterals/CVA-PT_March2016.pdf)

# NIST 800-30r1o

NIST 800-30r1 establishes a systematic process for assessing and managing risk by analyzing threat sources, vulnerabilities, and security controls to determine potential impacts on an organization. By applying this structured approach, organizations can proactively identify risks, prioritize security investments, and enhance overall cybersecurity resilience.

# Security architects think about the interactions among threats, vulnerabilities, impacts and risks



Here's a breakdown of the key components in **NIST 800-30r1**, each with a short description:

- 1.Threat Source** – The entity (e.g., hacker, insider, natural disaster) that has the capability, intent, or targeting to cause harm.
- 2.Threat Event** – The actual occurrence or scenario where a threat attempts to exploit a weakness in the system.
- 3.Vulnerability** – A weakness in a system, process, or control that a threat event can exploit to cause damage.
- 4.Security Controls** – Safeguards (technical, administrative, physical) designed to reduce the likelihood or impact of a successful attack.
- 5.Adverse Impact** – The negative consequences (e.g., data loss, system downtime, reputational damage) that result from a successful attack exploiting a vulnerability.

Each component **connects logically** in the risk assessment process, ultimately contributing to **organizational risk**

- Risk is the **likelihood** that a **threat** will exploit a **vulnerability**, causing damage to an organization.
- NIST emphasizes risk as a function of **threats**, **vulnerabilities**, **impact**, and **likelihood**.
- Organizations must continuously **assess**, **mitigate**, and **monitor** risks.

# What is a Risk?

## *A measure of threat*

*Potential loss resulting from unauthorized:*

- *Access, use, disclosure*
- *Modification*
- *Disruption or destruction*

*...of an enterprises' information*

*Can be expresses in **quantitative** and **qualitative** terms*

# Steps in a risk assessment methodology based on NIST 800-30r1

Step	Description
1. Prepare for the Risk Assessment	Define scope, purpose, methodology, and assets at risk.
2. Identify Threat Sources and Events	Identify adversarial and non-adversarial threats that could exploit vulnerabilities.
3. Identify Vulnerabilities and Predisposing Conditions	Identify weaknesses in security controls and conditions that increase risk.
4. Determine the Likelihood of Occurrence	Assess the probability of a threat successfully exploiting a vulnerability.
5. Determine the Magnitude of Impact	Analyze the potential damage and consequences of an incident.
6. Determine the Risk Level	Determine risk level by combining likelihood and impact.
7. Identify and Evaluate Security Controls	Identify preventive, detective, and corrective security controls.
8. Develop a Risk Response Strategy	Decide on risk response: accept, mitigate, transfer, or avoid the risk.
9. Monitor and Review the Risk Environment	Continuously assess, update risk strategies, and adapt to evolving threats.

There are two primary approaches to risk assessment:

- 1. Quantitative Risk Assessment** – Uses numerical values and statistical methods to estimate risk.
- 2. Qualitative Risk Assessment** – Uses descriptive scales (such as high, medium, low) to estimate risk based on expert judgment.



# Assessing risk – quantitative method

**Risk Calculation:** Uses formulas to calculate Single Loss Expectancy (SLE), Annualized Rate of Occurrence (ARO), and Annualized Loss Expectancy (ALE).

1. **Estimate potential losses (SLE)**—This step involves determining the single loss expectancy (SLE). SLE is calculated as follows:

— **Single loss expectancy (SLE) = Asset value X Exposure factor**

Items to consider when calculating the SLE include the physical destruction or theft of assets, the loss of data, the theft of information, and threats that might cause a delay in processing. The exposure factor is the measure or percent of damage that a realized threat would have on a specific asset.

2. **Conduct a threat analysis (ARO)**—The purpose of a threat analysis is to determine the likelihood of an unwanted event. The goal is to estimate the **annual rate of occurrence (ARO)**. Simply stated, **how many times is this expected to happen in one year?**

3. **Determine annual loss expectancy (ALE)**—This third and final step of the quantitative assessment seeks to combine the potential loss and rate per year to determine the magnitude of the risk. This is expressed as annual loss expectancy (ALE). ALE is calculated as follows:

— **Annualized loss expectancy (ALE) = Single loss expectancy (SLE) X Annualized rate of occurrence (ARO)**

## Examples of Calculations:

**Single Loss Expectancy (SLE)** = Asset Value (AV) × Exposure Factor (EF)

**Annualized Rate of Occurrence (ARO)** = Frequency of occurrence per year

**Annualized Loss Expectancy (ALE)** = SLE × ARO

### Example Calculation:

- A company's server is valued at \$100,000.
- A cyberattack has a 30% impact on the asset (EF = 0.3).
- The likelihood of the attack happening once every 5 years (ARO = 1/5 = 0.2).

$$SLE = 100,000 \times 0.3 = 30,000$$

$$ALE = 30,000 \times 0.2 = 6,000$$

This means the company can expect an annualized loss of \$6,000 due to this threat.

# Assessing risk – qualitative method

Qualitative risk assessment relies on subjective analysis using experience, expert judgment, and predefined risk matrices.

## Key Features:

- Uses **descriptive scales** (High, Medium, Low).
- Does **not** provide numerical values but offers relative risk rankings.
- Often uses **risk matrices** and heat maps to visualize risk levels.

## Alignment to NIST 800-30r1:

- **Likelihood and Impact Assessment:** Uses qualitative descriptors (e.g., "Moderate," "Severe").
- **Risk Prioritization:** Helps organizations **categorize risks** based on impact and likelihood.
- **Threat Identification:** Maps threats and vulnerabilities to qualitative risk levels

## Example:

A company assesses the risk of **phishing attacks**:

- **Likelihood:** "High" (occurs frequently).
- **Impact:** "Moderate" (leads to minor financial losses).
- **Risk Level:** "High" (based on a risk matrix).

While it lacks precision, **qualitative assessment is useful for initial risk identification** and when numerical data is unavailable.

# What is NIST?

- Non-regulatory agency of the United States Department of Commerce
- Measurement standards laboratory

**Mission:** *Promote innovation and industrial competitiveness*

***NIST is responsible for developing standards, guidelines, and associated methods and techniques for providing adequate information security for all agency operations and assets (excluding national security systems)***

# FIPS 199: Risk assessment based on security objectives and impact ratings

	POTENTIAL IMPACT		
Security Objective	LOW	MODERATE	HIGH
<b><i>Confidentiality</i></b> Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a <b>limited</b> adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a <b>serious</b> adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a <b>severe or catastrophic</b> adverse effect on organizational operations, organizational assets, or individuals.
<b><i>Integrity</i></b> Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a <b>limited</b> adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a <b>serious</b> adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a <b>severe or catastrophic</b> adverse effect on organizational operations, organizational assets, or individuals.
<b><i>Availability</i></b> Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a <b>limited</b> adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a <b>serious</b> adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a <b>severe or catastrophic</b> adverse effect on organizational operations, organizational assets, or individuals.

# Agenda

- ✓ Terminology
- ✓ Threat environment
- ✓ More terminology
- Security architecture
- Next steps...

# Implement the Operating Model Via Enterprise Architecture

**Enterprise Architecture (EA)** as a Framework: EA provides a structured approach for designing an enterprise's operations, ensuring that business processes, applications, and infrastructure align with corporate goals.

**The Role of the Operating Model:** The operating model defines how a company organizes processes, data, and technology to deliver value to customers and stakeholders.

**Components of EA:** The EA framework is divided into four key architectures:

- Information Architecture (Data Management)
- Business Architecture (Processes & Organizational Structure)
- Application Architecture (Software Systems & Integration)
- Infrastructure Architecture (Hardware, Networks & Cloud)



## Comparison of the Architectures

Architecture Type	Focus Area	Key Elements	Security Considerations
Information Architecture	Data management	Data lakes, governance, metadata	Data encryption, access control, backups
Business Architecture	Organizational processes	Workflows, capabilities, roles	Identity management, compliance frameworks
Application Architecture	Software applications & integration	APIs, microservices, software platforms	Secure coding, API security, app firewalls
Infrastructure Architecture	Physical & cloud infrastructure	Servers, cloud, networking, security layers	Firewalls, Zero Trust, endpoint security

# Security Architecture

A **Security Architecture** is a structured framework that ensures the **confidentiality, integrity, and availability (CIA)** of an enterprise's systems, data, and infrastructure.

It is integrated across all layers of **Enterprise Architecture (EA)** and includes strategic security controls, policies, and technologies.

# Security Architecture

“...the art and science of designing and supervising the construction of business systems, usually business information systems, which are:

- Free from danger, damage, etc.
- Free from fear, care, etc.
- In safe custody
- Not likely to fail
- Able to be relied upon
- Safe from attack”

Sherwood et al. (2005) Enterprise Security Architecture: A Business-Driven Approach

# Defenders must be perfect

*“One mistake by the defender essentially renders the whole defense worthless”*

*...every computer and software program must be patched, every configuration appropriately secure, and every end-user perfectly trained. Or at least that is the goal.*

*The defender knows that applied defenses may not always work or be applied as instructed, so they create “defense-in-depth” layers.”*

Grimes, R. (2017), Hacking the Hacker, John Wiley and Sons

# Security Architecture

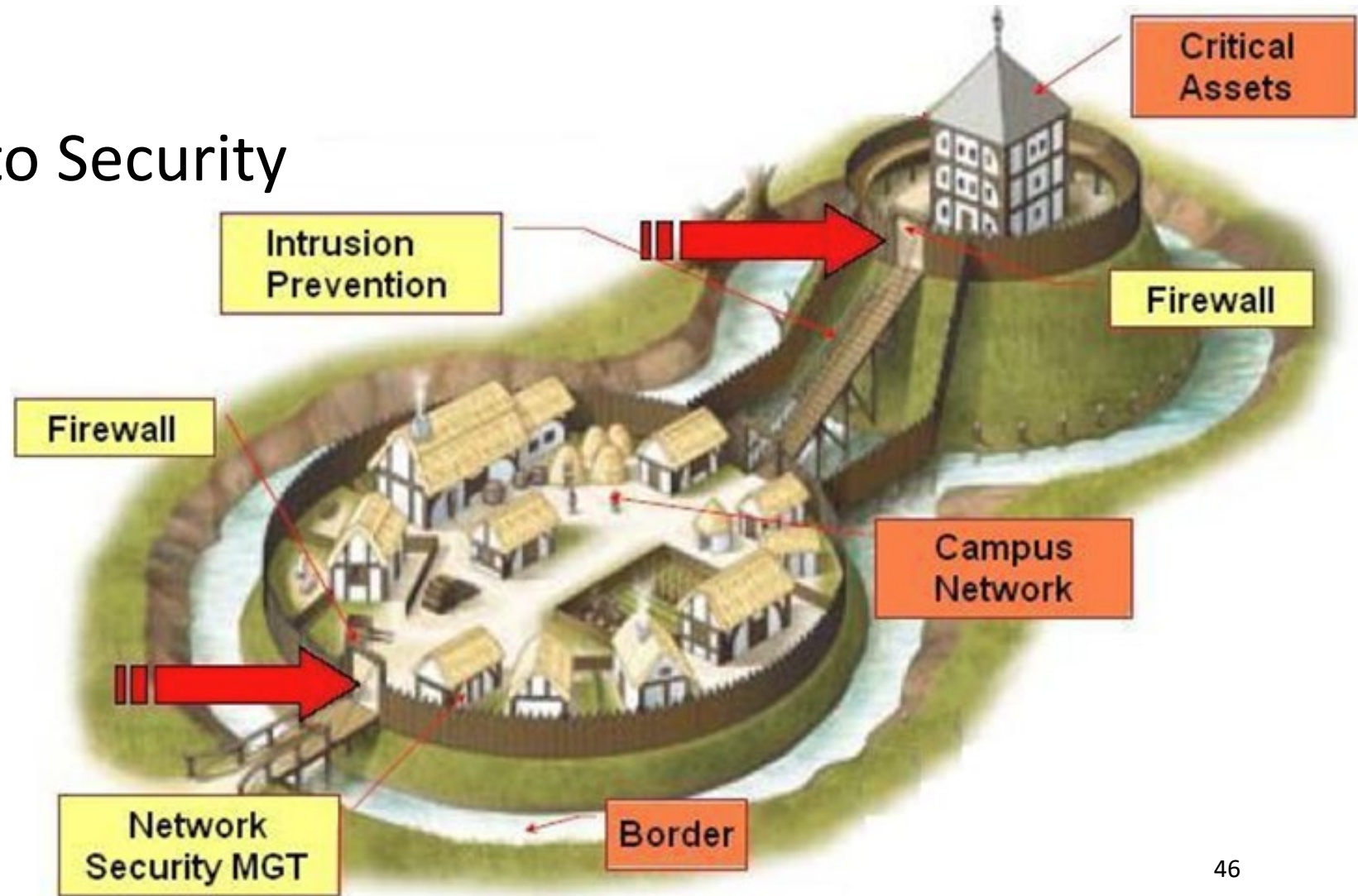
*Thinking about security architecture enables understanding enterprise information systems the way attackers do – as large diverse attack surfaces*



<https://graquantum.com/blog/cyber-basics-cyber-attack-surface/>

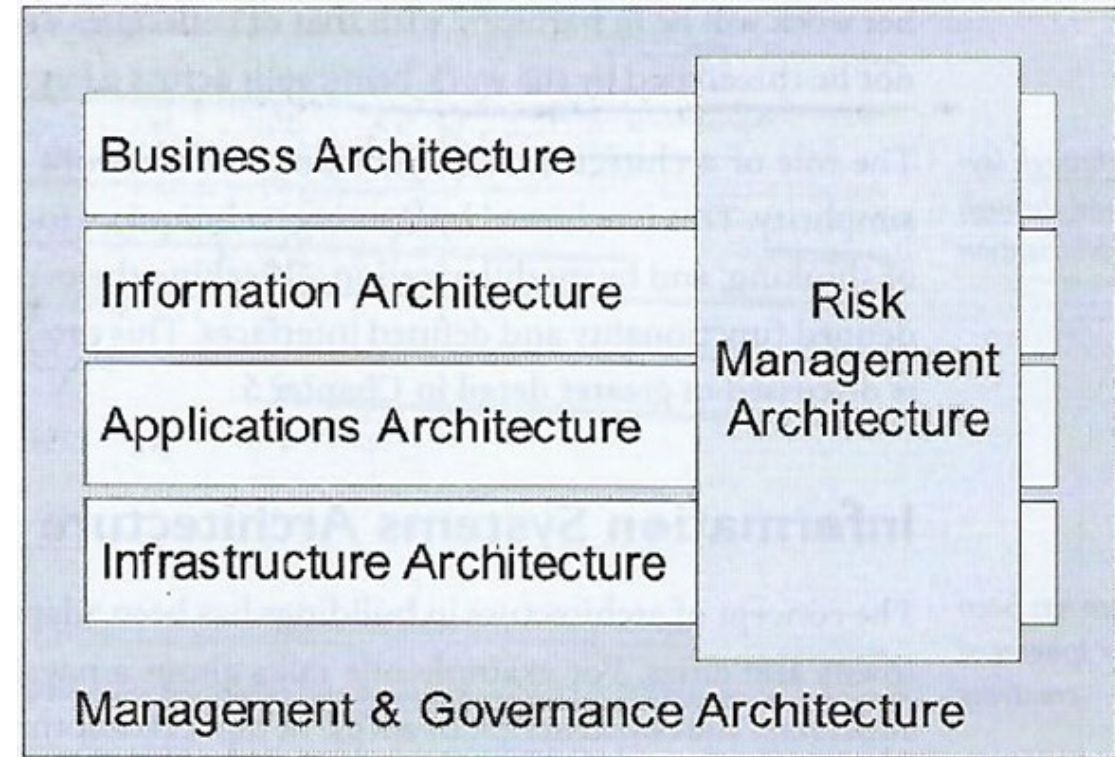
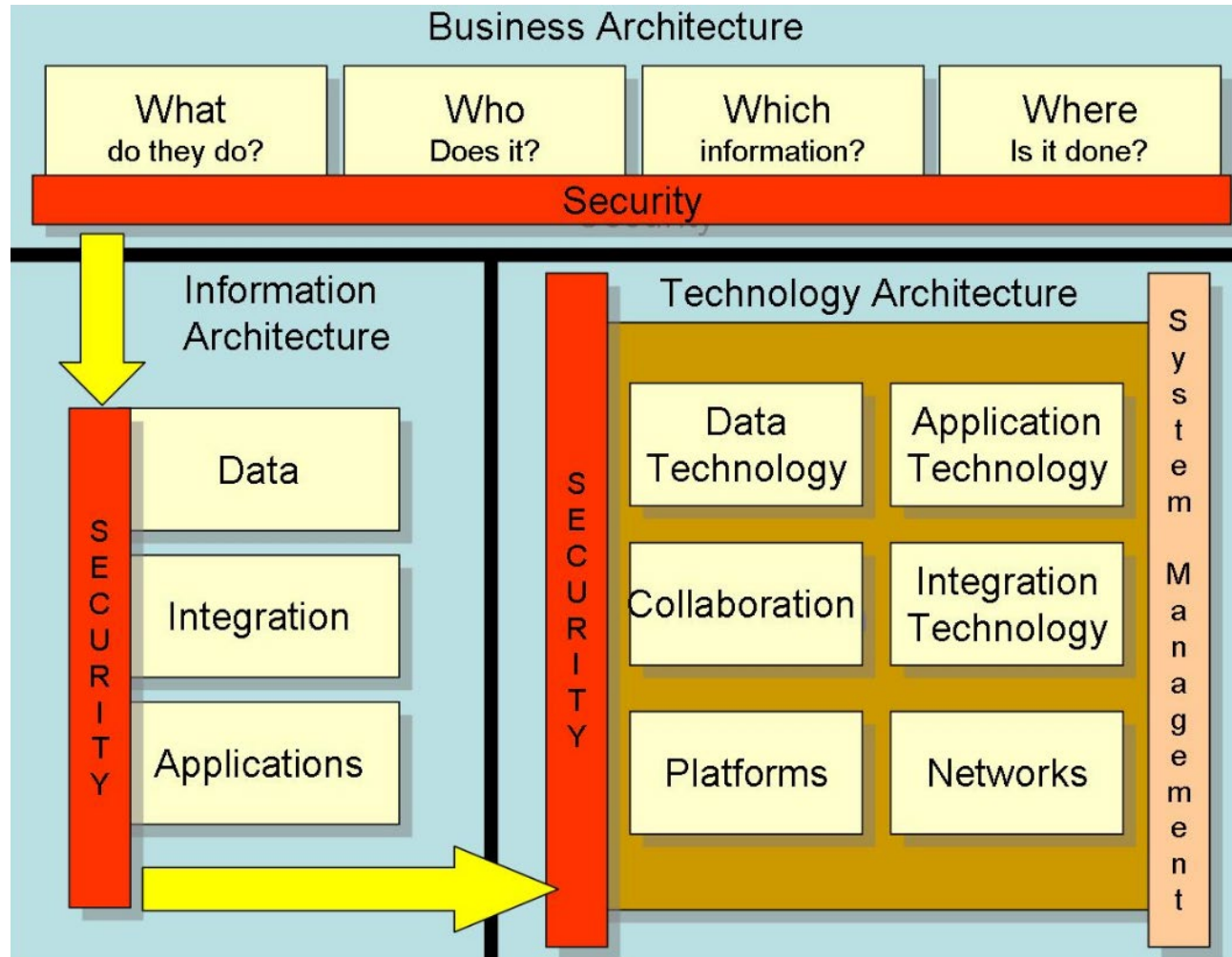
# Defense in Depth

- Also known as:
  - Layered Security
  - Castle Approach to Security





# Enterprise Information and Security Architecture



Sherwood et al. (2005) Enterprise Security Architecture: A Business-Driven Approach

Security Component	Function	Security Measures	Related Enterprise Architecture
Security Governance & Policies	Establishes security frameworks, risk management, compliance	IAM, NIST, ISO 27001, CIS Controls, role-based access control (RBAC)	Business Architecture
Network Security Architecture	Protects network traffic, prevents unauthorized access	Firewalls, IDS/IPS, VPNs, micro-segmentation, Zero Trust	Infrastructure Architecture
Data Security Architecture	Ensures data confidentiality, integrity, and availability	Encryption, DLP, tokenization, access controls, backups	Information Architecture
Application Security Architecture	Secures software applications, APIs, and web services	Secure SDLC, DevSecOps, WAF, MFA, API security, pen-testing	Application Architecture
Endpoint & Cloud Security	Protects devices, cloud environments, and user access	EDR, antivirus, patch management, CSPM, SASE, Zero Trust	Infrastructure & Application Architecture
Security Monitoring & Incident Response	Detects threats, monitors logs, and responds to incidents	SIEM, threat intelligence, behavioral analytics, SOC	Infrastructure & Business Architecture
Physical Security	Protects hardware, data centers, and physical access	CCTV, biometric authentication, facility security, access control	Infrastructure Architecture



# Next steps...

## Unit 1a – System Security Plan

### Readings

- [NIST SP 800-18r1 "Guide for Developing Security Plans for Federal Information Systems"](#)
- [FedRAMP System Security Plan \(SSP\) Low Moderate High Baseline Master Template](#)
- [FIPS Pub 199 Standards for Security Categorization of Federal Information and Information Systems](#)

# Agenda

- ✓ Terminology
- ✓ Threat environment
- ✓ Hacker mindset
- ✓ More terminology
- ✓ Security architecture
- ✓ Next steps...